

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-116029

(43)公開日 平成10年(1998) 5月6日

(51)Int.Cl.⁴
G 0 9 C 1/00

識別記号
6 1 0

F I
G 0 9 C 1/00

6 1 0 A
6 1 0 B

審査請求 未請求 請求項の数4 O L (全 7 頁)

(21)出願番号 特願平8-269897

(22)出願日 平成8年(1996)10月11日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 佐野 文彦

福岡県福岡市東区宮松3-7-25 木栄荘
201号

(72)発明者 櫻井 幸一

福岡県福岡市城南区七隈2-16-22

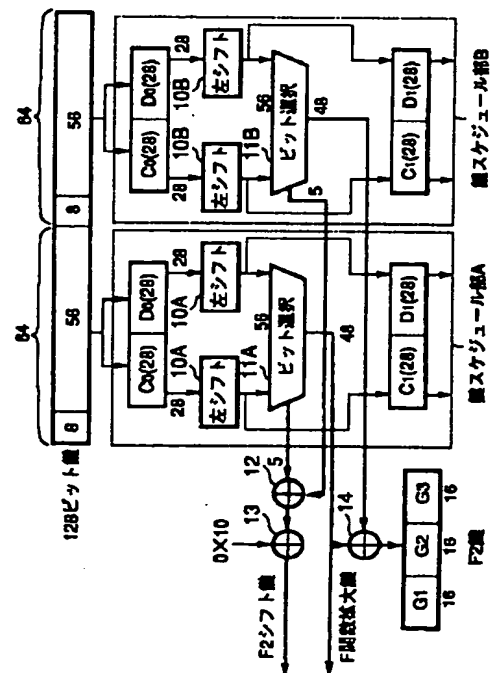
(74)代理人 弁理士 鈴江 武彦 (外6名)

(54)【発明の名称】 暗号化装置及び暗号化方法

(57)【要約】

【課題】DESとの互換性を維持しつつ安全性を増大することができる暗号化装置を提供する。

【解決手段】所定のビット列からなる鍵情報を等分して得られる2つの暗号化鍵を、入力電文を攪拌するのに用いられる中間鍵にそれぞれ展開する同一構成の2つの鍵スケジュール部A、Bと、この2つの鍵スケジュール部A、Bから出力された2つの中間鍵に対して排他的論理和を求める排他的論理和14と、この排他的論理和が0となることにより2つの中間鍵が互いに同一であることが検出された場合には、いずれか1つの中間鍵を用いて入力電文を攪拌するとともに、比較された2つの中間鍵が互いに同一でないことが検出された場合には、2つの中間鍵に基づいて入力電文を攪拌する攪拌部とを具備する。



1

【特許請求の範囲】

【請求項1】 入力電文を外部から入力された鍵情報に依存して攪拌し、対応する符号化電文を出力するデータ攪拌部と、

前記鍵情報を前記データ攪拌部に供給される中間鍵に展開する鍵スケジュール部とからなる暗号化装置であって、

前記鍵スケジュール部は、鍵情報の半数のビットを一意的出力に対応づける鍵展開手段と、

外部から入力された前記鍵ビットの内、半数を前記鍵展開手段にて第1の中間鍵に展開すると共に、全鍵ビットの残りの半数に同じ処理を施して第1の中間鍵と同数のビットからなる第2の中間鍵に展開し、該第2の中間鍵と第1の中間鍵のビット毎に所定の演算を行なうことにより、第3の中間鍵を得る手段とを有し、

前記データ攪拌部は、

前記第1乃至第3の中間鍵の一部または全部のビットの値によって規定される攪拌処理を実現する複数の攪拌手段を有し、

前記複数の攪拌手段の内、第3の中間鍵のみによって規定される攪拌手段は、第3の中間鍵のビットの内、前記攪拌手段で用いられているビットが特定の条件を満たした場合には、前記攪拌手段への入力ビット列と同一のビット列を出力するように構成されていることを特徴とする暗号化装置。

【請求項2】 所定のビット列からなる鍵情報を複数個に分割して得られる複数の暗号化鍵を、入力電文を攪拌するのに用いられる中間鍵にそれぞれ展開する同一構成の複数の鍵展開手段と、

この複数の鍵展開手段から出力された複数の中間鍵を互いに比較する比較手段と、

この比較手段によって比較された複数の中間鍵が同一であることが検出された場合には、複数の中間鍵のいずれか1つを用いて入力電文を攪拌するとともに、

比較された複数の中間鍵が同一でないことが検出された場合には、複数の中間鍵のすべてに基づいて入力電文を攪拌する攪拌手段と、

を具備することを特徴とする暗号化装置。

【請求項3】 外部から入力された鍵情報を鍵スケジュール部において中間鍵に展開し、データ攪拌部においてこの中間鍵に依存して入力電文を攪拌して対応する符号化電文を出力する暗号化方法であって、

所定の鍵展開手段によって、外部から入力された鍵情報の内、半数のビットを第1の中間鍵に展開すると共に、前記鍵情報の残りのビットに同じ処理を施して第1の中間鍵と同数のビットからなる第2の中間鍵に展開し、さらに、第1の中間鍵と第2の中間鍵との間でビット毎に所定の演算を行なうことにより、第3の中間鍵を得るとともに、

2

前記第1、第2、第3の中間鍵の一部または全部のビットの値によって規定される攪拌処理を行なうにあたって、第3の中間鍵のみによって規定される攪拌処理は、第3の中間鍵が特定の条件を満たした場合には、入力ビット列と同一のビット列を出力することを特徴とする暗号化方法。

【請求項4】 同一構成の複数の鍵展開手段によって、所定のビット列からなる鍵情報を複数個に分割して得られる複数の暗号化鍵を入力電文を攪拌するのに用いられる中間鍵にそれぞれ展開する展開工程と、

前記複数の鍵展開手段から出力された複数の中間鍵を互いに比較する比較工程と、

この比較工程において比較された複数の中間鍵が同一であることが検出された場合には、複数の中間鍵のいずれか1つを用いて入力電文を攪拌するとともに、

比較された複数の中間鍵が同一でないことが検出された場合には、複数の中間鍵のすべてに基づいて入力電文を攪拌する攪拌工程と、

を具備することを特徴とする暗号化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は暗号化装置及び暗号化方法に関し、特に、秘密鍵ブロック暗号を用いた暗号化装置及び暗号化方法に関する。

【0002】

【従来の技術】 DES (Data Encryption Standard)

は、現在、最も広範に用いられている秘密鍵ブロック暗号系であり、文献、"Data Encryption Standard," Federal Information Processing Standards Publication 46, National Bureau of Standards, U.S. Department of Commerce, 1977. に詳細に記載されている。

【0003】 DESは64ビット入力、64ビット出力のブロック暗号であり、そのうち8ビットは鍵パリティ用として使用されるので56ビットのみが実質的な鍵である。したがって、DESが開発された当初からその安全性について議論がなされており、1977年に発表されて以来、さまざまな観点からの評価が行われている。その結果、1990年ごろに差分解読法や線形解読法といった鍵の全数探索よりも効率的な解読法が次々と提案された。特に、線形解読法を用いることにより、標準である16段DESの解読に成功している。

【0004】 なお、差分解読法については、文献、E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of CRYPTOLOGY, Vol. 4, Number 1, 1991に、線形解読法については、文献、松井充, "DES暗号の線形解読 (I)", 暗号と情報セキュリティシンポジウム, SCIS93-3C, 1993に記載されている。

【0005】 DESが開発されてからの技術の発展や上記したような解読法を考慮すると、DESには以下のよ

3

うな問題点があると考えられる。

(1) 現在のハードウェア技術の進歩を考えると処理を高速に行なうために128ビットのブロック暗号を構成することが可能であるが、いぜんとして64ビットのブロック暗号を用いている。

(2) F関数の構造に問題がある。DESが開発された当時では、線形解読法が発案されておらず、線形解読法に対する耐性が考慮されていない。また、ハードウェア技術の発達への制約からF関数に含まれるS箱のテーブルサイズが小さい。現在のハードウェア技術のレベルを考えるとS箱のサイズをより大きくして安全性を高めることが望ましい。

(3) 56ビットからなる鍵を用いているが、56ビットの鍵の長さでは安全ではない。ハードウェアの発達により、現在では2⁵⁶個の鍵の組合せを調べるハードウェアの実現が可能である。また、専用のハードウェアを用いることにより、鍵の全数探索が可能であるとの発表もなされている。また、DESの解読方法の1つである線形解読法は、鍵の一部のビットを解読により特定して残りのビットに対して全数探索を行なうものであるから、鍵を増やすことにより残りの鍵ビットの全数探索を行なう手間が増大して安全性が向上すると考えられる。

【0006】上記した問題において、(3)のDESの鍵の長さに関する問題については、DESチップをそのまま使用しながら鍵を長くする方法が考えられている。例えば、論文、B.Schneier, "Applied Cryptography," 2nd edition, Wiley (1996)は、DESXやTripleDESなどの暗号化方法を開示している。

【0007】DESXはDESの入力及び出力の各々と64ビットの鍵との排他的論理和をとる方法であるが、鍵の全数探索に対しては理論的な安全性が証明されている(J.Kilian and P.Rogaway, "How to protect DES against exhaustive key search," Proc. CRYPTO'96, p.252-267(1996)を参照)。また、TripleDESはDESを3重に処理するアルゴリズムを用いているので、鍵の全数探索だけでなく、差分解読法や線形解読法に対しても、DES以上の安全性が確保できる。

【0008】

【発明が解決しようとする課題】しかしながら、上記したDESXは差分解読法や線形解読法に対してはDESと同等の安全性しか達成されない。また、TripleDESは構成が3倍になるので、処理速度はDESの処理速度の1/3となる。

【0009】一方、上記した(1)、(2)で述べた問題点はDESの構造自体に関しており、これらを改良することは容易でない。また、これらを改良すれば本体のDESとは異なった暗号化処理を行なうことになり、DESとの互換性の問題が新たに発生してしまう。

【0010】本発明の暗号化装置及び暗号化方法はこのような課題に着目してなされたものであり、その目的と

4

するところは、DESとの互換性を維持しつつ安全性を増大することができる暗号化装置及び暗号化方法を提供することにある。

【0011】

【課題を解決するための手段】上記の目的を達成するために、第1の発明に係る暗号化装置は、入力電文を外部から入力された鍵情報に依存して攪拌し、対応する符号化電文を出力するデータ攪拌部と、前記鍵情報を前記データ攪拌部に供給される中間鍵に展開する鍵スケジュール部とからなる暗号化装置であって、前記鍵スケジュール部は、鍵情報の半数のビットを一意的出力に対応づける鍵展開手段と、外部から入力された前記鍵ビットの内、半数を前記鍵展開手段にて第1の中間鍵に展開すると共に、全鍵ビットの残りの半数に同じ処理を施して第1の中間鍵と同数のビットからなる第2の中間鍵に展開し、該第2の中間鍵と第1の中間鍵のビット毎に所定の演算を行なうことにより、第3の中間鍵を得る手段とを有し、前記データ攪拌部は、前記第1乃至第3の中間鍵の一部または全部のビットの値によって規定される攪拌処理を実現する複数の攪拌手段を有し、前記複数の攪拌手段の内、第3の中間鍵のみによって規定される攪拌手段は、第3の中間鍵のビットの内、前記攪拌手段で用いられているビットが特定の条件を満たした場合には、前記攪拌手段への入力ビット列と同一のビット列を出力するように構成されている。

【0012】また、第2の発明に係る暗号化装置は、所定のビット列からなる鍵情報を複数個に分割して得られる複数の暗号化鍵を入力電文を攪拌するのに用いられる中間鍵にそれぞれ展開する同一構成の複数の鍵展開手段と、この複数の鍵展開手段から出力された複数の中間鍵を互いに比較する比較手段と、この比較手段によって比較された複数の中間鍵が同一であることが検出された場合には、複数の中間鍵のいずれか1つを用いて入力電文を攪拌するとともに、比較された複数の中間鍵が同一でないことが検出された場合には、複数の中間鍵のすべてに基づいて入力電文を攪拌する攪拌手段とを具備する。

【0013】また、第3の発明に係る暗号化方法は、外部から入力された鍵情報を鍵スケジュール部において中間鍵に展開し、データ攪拌部においてこの中間鍵に依存して入力電文を攪拌して対応する符号化電文を出力する暗号化方法であって、所定の鍵展開手段によって、外部から入力された鍵情報の内、半数のビットを第1の中間鍵に展開すると共に、前記鍵情報の残りのビットに同じ処理を施して第1の中間鍵と同数のビットからなる第2の中間鍵に展開し、さらに、第1の中間鍵と第2の中間鍵との間でビット毎に所定の演算を行なうことにより、第3の中間鍵を得るとともに、前記第1、第2、第3の中間鍵の一部または全部のビットの値によって規定される攪拌処理を行なうにあたって、第3の中間鍵のみによって規定される攪拌処理は、第3の中間鍵が特定の条件

5

を満たした場合には、入力ビット列と同一のビット列を出力する。

【0014】また、第4の発明に係る暗号化方法は、同一構成の複数の鍵展開手段によって、所定のビット列からなる鍵情報を複数個に分割して得られる複数の暗号化鍵を入力電文を攪拌するのに用いられる中間鍵にそれぞれ展開する展開工程と、前記複数の鍵展開手段から出力された複数の中間鍵を互いに比較する比較工程と、この比較工程において比較された複数の中間鍵が同一であることが検出された場合には、複数の中間鍵のいずれか1つを用いて入力電文を攪拌するとともに、比較された複数の中間鍵が同一でないことが検出された場合には、複数の中間鍵のすべてに基づいて入力電文を攪拌する攪拌工程とを具備する。

【0015】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態を詳細に説明する。図1は本実施形態に係る暗号化装置の構成を示す図であり、入力電文としての平文（64ビット）を外部から入力された鍵情報kに依存して攪拌し、対応する符号化電文を出力する第1段～第16段から構成されるデータ攪拌部と、鍵情報kを前記データ攪拌部に供給される中間鍵に展開する鍵スケジュール部4とからなる。

【0016】図1において、平文（64ビット）は初期転置IPが施された後、2つに等分されて左側32ビットL₀と右側32ビットR₀が生成される。一方、鍵スケジュール4には128ビットの鍵情報kが入力される。鍵スケジュール4は以下に述べる方法によってF関数拡大鍵とF2鍵及びF2シフト鍵を生成して、データ攪拌部のF関数2とF2関数3にそれぞれ入力する。ここでF関数2は通常のDESと同様の攪拌処理を行なうものであり、F2関数3は以下に述べるような攪拌処理を行なう。

【0017】F関数2はF関数拡大鍵とF2関数3の出力とを受けて所定の攪拌処理を行ってその結果を排他的論理和1に入力する。排他的論理和1はL₀（32ビット）とF関数2の出力との間の排他的論理和を出力するが、これによって次段の右側32ビットR₁が得られる。また、F2関数3の出力は次段の左側32ビットL₁となる。

【0018】以上の攪拌処理が第1段で行われ、L₁（32ビット）とR₁（32ビット）とが第2段に送られて第1段と同様の処理が施される。このようにして第16段までの攪拌処理が行われた後、最終転置IP⁻¹が施されて暗号文（64ビット）が得られる。

【0019】このように本実施形態では、DESの各段で使用される鍵のビット数を増加させるために、通常のDESの構成に加えて、各段の入力側（図1に示す位置）にF2関数を組み込んでいる。

【0020】図2は図1に示す鍵スケジュール部4の1

6

段分の構成を示しており、DESと同一の構成の鍵スケジュール部Aと鍵スケジュール部Bとからなる。したがって鍵スケジュール部4はこのような構成の鍵スケジュール部を16段設けた構成を有する。鍵スケジュール部A、Bとも同一の処理を行なうのでここでは鍵スケジュール部Aについてのみ説明する。

【0021】128ビットの鍵情報は半分ずつに分割され、縮約型転置PC-1を施された後、56ビットの鍵として各々の鍵スケジュール部に入力される。鍵（56ビット）を2つに等分して生成した28ビットからなる2つの鍵の各々C₀（28ビット）、D₀（28ビット）について左シフト部10Aで左シフト処理を施した後、ビット選択部11Aに入力する。ビット選択部11Aは所定のビット選択処理により48ビットからなる第1の中間鍵と、5ビットからなる鍵とを出力する。この5ビットの鍵としては、56ビット鍵の例えば、左から9、18、22、25、35番目の5ビットが用いられる。同様にビット選択部10Bからは48ビットからなる第2の中間鍵と、5ビットからなる鍵とが出力される。

【0022】そして、ビット選択部11Aからの48ビットの鍵とビット選択部11Bからの48ビットの鍵との間で排他的論理和14をとり、その結果としての48ビットの第3の中間鍵を3等分して16ビットの鍵G₁、G₂、G₃を得る。この鍵G₁、G₂、G₃をF2鍵としてF2関数3に入力する。

【0023】同様に、鍵スケジュール部Aのビット選択部11Aからの5ビットの鍵と、鍵スケジュール部Bのビット選択部11Bからの5ビットの鍵との間で排他的論理和12を求め、その結果と0X10（0Xは16進を表す）との間で排他的論理和13をとったものをF2シフト鍵としてF2関数3に入力する。

【0024】さらに、本実施形態では、鍵スケジュール部Aのビット選択部11Aからの48ビットの鍵をF関数拡大鍵としてF関数2に入力する。また、各々の28ビットの鍵C₀（28ビット）、D₀（28ビット）を左シフトすることによって得られたC₁（28ビット）、D₁（28ビット）は次の段の鍵スケジュール部の入力となる。

【0025】このように本実施形態では、DESとの互換性を維持するために、128ビットの鍵を64ビットずつに分割し、それぞれに対してDESの鍵スケジュール部A、Bを適用している。また、F関数に入力される拡大鍵としては鍵スケジュール部Aからの48ビットの鍵をそのまま用いている。また、F2関数に用いる鍵としては鍵スケジュール部Aからの48ビット鍵と鍵スケジュール部Bからの48ビット鍵とのビットごとの排他的論理和を16ビットごとのブロックに分割して、それぞれG₁、G₂、G₃としている。また、56ビット鍵の左から特定番目の5ビットを選択してF2関数のシフ

7

ト鍵として用いている。

【0026】図3はF2関数3の構成を示す図である。ここでは図1に示すR0（32ビット）を2つに等分して2つの16ビットのブロックを生成する。左側の16ビットブロックは排他的論理和20にされる。また、右側の16ビットブロックは論理積21と排他的論理和22にされる。

【0027】論理積21は16ビット鍵G1と右側の16ビット鍵との論理積をとって排他的論理和20にする。排他的論理和20は左側の16ビットブロックと論理積21からの鍵との間で排他的論理和を取り、その結果を左巡回シフト部23にする。

【0028】一方、排他的論理和22は16ビット鍵G2と右側の16ビットブロックとの間で排他的論理和を取り、その結果を左巡回シフト部23にする。左巡回シフト部23は、排他的論理和20の出力と排他的論理和22の出力からなる32ビットの鍵に対して、された5ビットのF2シフト鍵を2進表記とみなして、そのビット数分の左巡回シフトを行なう。

【0029】左巡回シフトを行った後の32ビットの中間データの左半分の16ビットはF2関数3の右半分の出力となる。また、左巡回シフトを行った後の32ビットの中間データの右半分の16ビットは排他的論理和24にされる。

【0030】論理積25は16ビットの鍵G3と左巡回シフトを行った後の32ビットの中間データの左半分の16ビットとの論理積をとってその結果を排他的論理和24にする。排他的論理和24はこの論理積と左巡回シフトを行った後の32ビットの中間データの右半分の16ビットとの間の排他的論理和を取り、その結果をF2関数3の左半分として出力する。

【0031】上記したように、本実施形態のF2関数では、32ビットの入力を16ビットずつに分割して、分割された鍵とのビットごとの論理和や論理積をとっている。また、巡回シフト部ではF2シフト鍵のビット数だけ32ビットの鍵に対して巡回シフトを行っている。

【0032】以上の説明からわかるように、本実施形態の暗号化装置の利点はDESと同一の鍵スケジュール構成を用いていることにある。64ビットの鍵を複製して128ビットの鍵を生成することにより、DESとの完全な互換性を維持することができる。なぜなら、2つの鍵スケジュール部A、Bの64ビットの入力が同じであるならば、各スケジュール部で生成される中間鍵も同一のものとなる。各スケジュール部で生成される中間鍵が同一ならば両者のビットごとの排他的論理和14は0となるため、F2関数3で用いられるG1、G2、G3も0となる。また同様に、排他的論理和12の出力も0となり、F2シフト鍵は0X10となる。

【0033】このとき、図3に示すF2関数3の排他的論理和20、22の一方の入力が0となるので、F2関

8

数3にされた2つの16ビットの鍵はそのまま左巡回シフト部23にされる。さらに、左巡回シフト部23では鍵スケジュール部A、Bからの2つの5ビット鍵の間の排他的論理和12と0X10との排他的論理和13をF2シフト鍵とし、このようなF2シフト鍵に基づいて左巡回を行っているので、G3=0、すなわち、排他的論理和24の一方の入力が0のときは、F2関数3にされたビット列（32ビット）と同じビット列が出力されることになる。

10 【0034】このようにして、2つの鍵スケジュール部A、Bの64ビットの入力が同じであるならば、F2関数3の構造は無視されることになるので、128ビット鍵の半分の64ビットを鍵として用いたDESと全く同じ処理となり、互換性が満足される。

【0035】さらに、本実施形態ではF2関数を加えたことによりDESと比較して各段でのデータ処理が増加することになるが、F2関数で用いられる演算は左巡回シフト命令、論理和、論理積、排他的論理和であり、これらの演算は通常多くのハードウェアに実装されているので高速処理が可能である。このことより、処理効率はDESと比較してあまり低下することはない。

20 【0036】また、本実施形態ではF2関数での鍵の加え方に工夫を行っている。鍵を加える場合、入力データと鍵との排他的論理和をとる方法があるが、この方法では線形解読法を適用したときに排他的論理和で加えられた鍵は解読の過程で比較的容易に導出されてしまい、鍵のビット数を増やしても安全性を高める効果が少ない。これに対して、本実施形態では、論理和や論理積を用いて鍵を加えているので、線形解読法による鍵の直接の導出は行われず、鍵のビット数の増加により強度の安全性の向上が計れる。

30 【0037】以下に、OSとしてSolaris2.5、コンパイラとしてgcc-2.7.2を用い、最適化オプションなしのシステム環境下で、本実施形態の暗号化用サンプルソースプログラムを実行した場合のスループットを本実施形態とDESについて計測した。ここでは、上記サンプルソースプログラムからF2関数に関する部分を取り除いたものをDESの構成としている。

40 【0038】計測の結果、図4（a）に示すような結果が得られた。スループットの速度比では本実施形態はDESの90.6%であり、DESを3重に構成したTripleDESがDESの1/3（すなわち、33.3%）の速度であることと比較して十分高速であることがわかる。

50 【0039】次に、OSとしてLinux、CPUとしてPentium 120MHz、コンパイラとしてgcc-2.7.2.1、最適化オプションとして-O2を用いたシステム環境下で同様のサンプルソースプログラムを実行した場合のスループットを本実施形態とDESについて計測した。この場合も上記サンプルソースプログラムからF2関数に関する部

分を取り除いたものをDESの構成としている。

【0040】計測の結果、図4(b)に示すような結果が得られた。図4(b)によれば、スループットの速度比では本実施形態はDESの65%であり、DESを3重に構成したTripleDESがDESの1/3の速度であることと比較してまだ十分高速であることがわかる。

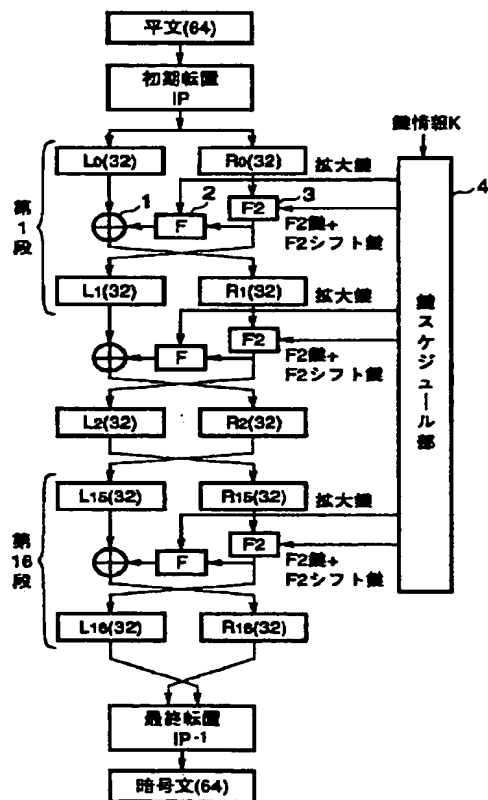
【0041】

【発明の効果】本発明によれば、DESとの互換性を維持しつつ安全性を増大することができる暗号化装置及び暗号化方法を提供できる。

【図面の簡単な説明】

【図1】本発明の一実施形態における暗号化装置の構成 *

【図1】



*を示す図である。

【図2】図1に示す鍵スケジュール部4の1段分の構成を示す図である。

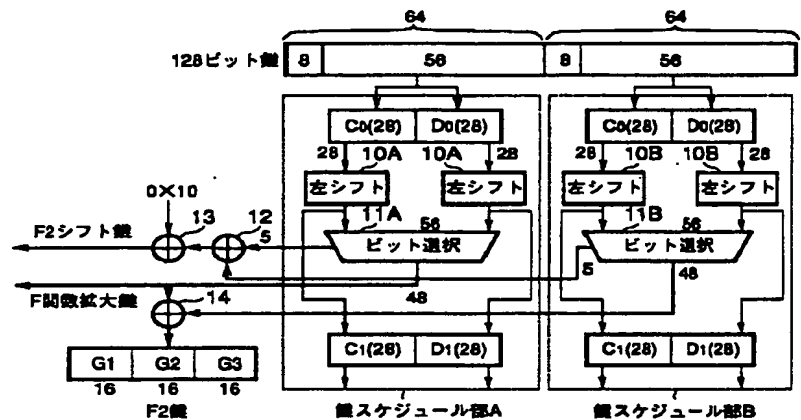
【図3】図1に示すF2関数の構成を示す図である。

【図4】本実施形態の暗号化方法に係るサンプルソースプログラムを実行した場合のスループットを本実施形態とDESについて計測した結果を示す図である。

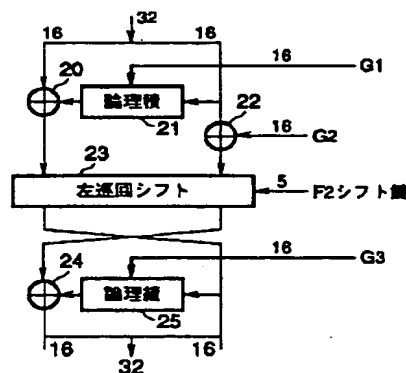
【符号の説明】

1…排他的論理和、2…F関数、3…F2関数、4…鍵スケジュール部、10A、10B…左シフト部、11A、11B…ビット選択部、12、13、14…排他的論理和。

【図2】



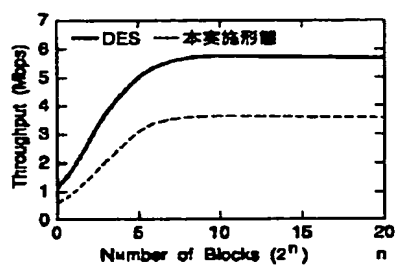
【図3】



【図 4】

DES	本実施形態	速度比
64Kbps	58Kbps	90.6%

(a)



(b)

THIS PAGE BLANK (USPTO)